# EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 2013/40/EU

## af 12. august 2013

## om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 83, stk. 1,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg [1],

efter den almindelige lovgivningsprocedure [2], og

ud fra følgende betragtninger:

(1) Dette direktivs formål er at tilnærme medlemsstaternes strafferet til hinanden med hensyn til angreb på informationssystemer ved at fastsætte minimumsregler for definitionen af strafbare handlinger og de relevante sanktioner og at forbedre samarbejdet mellem de kompetente myndigheder, herunder politiet og andre specialiserede retshåndhævende myndigheder i medlemsstaterne samt kompetente specialiserede EU-agenturer og -organer, som f.eks. Eurojust, Europol og dets europæiske center for bekæmpelse af it-kriminalitet og Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA).

(2) Informationssystemer er et centralt element i det politiske, sociale og økonomiske samspil i Unionen. Samfundet er dybt afhængigt af sådanne systemer og bliver det i stadig større udstrækning. Disse systemers funktionsdygtighed og sikkerhed i Unionen er en forudsætning for udviklingen af det indre marked og af en konkurrencedygtig og innovativ økonomi. Der bør sikres et passende beskyttelsesniveau for informationssystemer som led i en effektiv overordnet ramme for forebyggende foranstaltninger, der ledsager de strafferetlige foranstaltninger over for it-kriminalitet.

(3) Angreb på informationssystemer, og især angreb som led i organiseret kriminalitet, er en voksende trussel såvel i Unionen som globalt, og der er i stigende grad bekymring for mulige terrorangreb eller politisk motiverede angreb på informationssystemer, der indgår i medlemsstaternes og Unionens kritiske infrastruktur. Dette udgør en trussel mod etableringen af et sikrere informationssamfund og et område med frihed, sikkerhed og retfærdighed og kræver derfor en reaktion på EU-niveau samt bedre samarbejde og koordination på internationalt niveau.

(4) Der findes adskillige kritiske infrastrukturer i Unionen, hvis afbrydelse eller ødelæggelse ville få betydelige konsekvenser på tværs af grænserne. Det er blevet klart ud fra behovet for at øge Unionens evne til at beskytte kritisk infrastruktur, at foranstaltningerne mod it-angreb bør suppleres af strenge strafferetlige sanktioner, der afspejler disse angrebs alvorlige karakter. Kritisk infrastruktur kan forstås som aktiver, systemer eller dele deraf, der befinder sig i medlemsstaterne, og som er væsentlige for opretholdelsen af vitale samfundsmæssige funktioner, menneskers sundhed, sikkerhed og økonomiske eller sociale velfærd, såsom kraftværker, transportnetværk og statslige netværk, og hvis afbrydelse eller ødelæggelse i væsentlig grad ville påvirke en medlemsstat som følge af, at disse funktioner ikke kan opretholdes.

(5) Der er tegn på en tendens til stadig farligere og gentagne omfattende angreb på informationssystemer, der ofte kan være kritiske for medlemsstaterne eller for enkelte funktioner i den offentlige eller private sektor. Denne tendens falder sammen med udviklingen af stadigt mere avancerede metoder, f.eks. oprettelsen og anvendelsen af såkaldte botnet, der indebærer flere stadier af en strafbar handling, hvor hvert stadium i sig selv kan udgøre en alvorlig risiko for samfundets interesser. Dette direktiv sigter bl.a. mod at indføre strafferetlige sanktioner for oprettelse af botnet, dvs. den handling, som går ud på gennem målrettede it-angreb, at etablere fjernstyring af et betydeligt antal computere ved at inficere dem med skadelig software. Efter oprettelsen kan det inficerede netværk af computere, der udgør botnettet, aktiveres uden computerbrugerens vidende for at foretage et omfattende it-angreb, der som regel har kapacitet til at volde alvorlig skade, som omhandlet i dette direktiv. Medlemsstaterne bør kunne fastsætte, hvad der i henhold til deres nationale lovgivning og praksis udgør alvorlig skade, så som afbrydelse af systemtjenester med væsentlig betydning for offentligheden eller forårsagelse af store økonomiske omkostninger eller tab af personoplysninger eller følsomme oplysninger.

(6) Omfattende it-angreb kan forvolde alvorlig økonomisk skade, såvel gennem afbrydelsen af informationssystemer og kommunikationsstrømme som gennem tabet eller forvanskningen af kommercielt vigtig fortrolig information eller andre data. Der bør lægges særlig vægt på at gøre innovative små og mellemstore virksomheder bevidste om trusler i forbindelse med sådanne angreb og deres sårbarhed overfor sådanne angreb som følge af deres øgede afhængighed af velfungerende og tilgængelige informationssystemer og ofte begrænsede midler til informationssikkerhed.

[1] EUT C 218 af 23.7.2011, s. 130.

[2] Europa-Parlamentets holdning af 4.7.2013 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 22.7.2013.

(7) Fælles definitioner på dette område er vigtige for at sikre en ensartet tilgang i medlemsstaterne til anvendelsen af dette direktiv.

(8) Der er behov for at nå frem til en fælles tilgang til gerningsindholdet af strafbare handlinger ved at indføre fælles definitioner af strafbare handlinger med hensyn til ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer, ulovligt indgreb i data og ulovlig opfangning.

(9) Opfangning omfatter, men er ikke nødvendigvis begrænset til, aflytning, overvågning eller kontrol af kommunikationens indhold og fremskaffelse af dataindholdet enten direkte via adgang til og brug af informationssystemerne, eller indirekte via anvendelse af elektronisk aflytning eller aflytningsudstyr ved hjælp af tekniske hjælpemidler.

(10) Medlemsstaterne bør fastsætte sanktioner for angreb på informationssystemer. Disse sanktioner bør være effektive, stå i et rimeligt forhold til de strafbare handlingers grovhed og have afskrækkende virkning og bør omfatte fængsels- og/eller bødestraf.

(11) Dette direktiv fastsætter strafferetlige sanktioner i det mindste i grovere tilfælde. Medlemsstaterne kan beslutte, hvilke tilfælde der ikke er grove i henhold til deres nationale lovgivning og praksis. Et tilfælde kan betragtes som mindre groft, f.eks. når den skade og/eller den fare for offentlige eller private interesser, der forårsages af den strafbare handling, såsom på et computersystems eller computerdatas integritet eller på en persons integritet, rettigheder og andre interesser, er ubetydelig eller af en sådan karakter, at der ikke er behov for at pålægge en strafferetlig sanktion inden for straffelovgivningens rammer eller pålægge strafferetligt ansvar.

(12) Identifikation og indberetning af de trusler og risici, som it-angreb indebærer, og informationssystemers dermed forbundne sårbarhed er et vigtigt element i en effektiv forebyggelse af og reaktion på it-angreb og for forbedringen af informationssystemers sikkerhed. Incitamenter til at indberette sikkerhedsmangler kunne bidrage hertil. Medlemsstaterne bør bestræbe sig på at skabe muligheder for lovligt at afsløre sikkerhedsmangler og indberette dem.

(13) Det er hensigtsmæssigt at fastsætte strengere sanktioner, når det er en kriminel organisation som defineret i Rådets rammeafgørelse 2008/841/RIA af 24. oktober 2008 om bekæmpelse af organiseret kriminalitet [1], der har begået angrebet på informationssystemet, når it-angrebet er meget omfattende og dermed berører et betydeligt antal informationssystemer, herunder når angrebet har til formål at oprette et botnet, eller når et it-angreb volder alvorlig skade, herunder når det udføres ved hjælp af et botnet. Det er også hensigtsmæssigt at fastsætte strengere sanktioner, når der foretages et angreb på kritisk infrastruktur i medlemsstaterne eller Unionen.

(14) Indførelse af effektive foranstaltninger til bekæmpelse af identitetstyveri og andre identitetsrelaterede strafbare handlinger udgør et andet vigtigt element i en integreret strategi mod it-kriminalitet. Behov for EU-tiltag over for denne type kriminel adfærd kunne også overvejes i forbindelse med vurderingen af nødvendigheden af et omfattende horisontalt EU-instrument.

(15) Rådet anførte i sine konklusioner fra samlingen den 27.-28. november 2008, at der burde udvikles en ny strategi sammen med medlemsstaterne og Kommissionen, hvori der skulle tages hensyn til indholdet af Europarådets konvention om it-kriminalitet af 2001. Konventionen udgør den retlige referenceramme for bekæmpelse af it-kriminalitet, herunder angreb på informationssystemer. Dette direktiv bygger på konventionen. Det bør betragtes som en prioritet, at medlemsstaterne hurtigst muligt fuldfører konventionens ratifikationsproces.

(16) Under hensyn til de forskellige måder, hvorpå angreb kan foretages, og på grund af den hurtige udvikling i hardware og software, nævner dette direktiv værktøjer, som kan bruges til at begå de strafbare handlinger, der er opført i dette direktiv. Sådanne værktøjer kunne omfatte skadelig software, herunder værktøjer, der gør det muligt at oprette botnet, som bruges til at begå it-angreb. Selv om et sådant værktøj er egnet eller særligt egnet til at begå en af de i dette direktiv omhandlede strafbare handlinger, kan det være fremstillet til et lovligt formål. Drevet af behovet for at undgå kriminalisering i tilfælde, hvor sådanne værktøjer fremstilles og markedsføres til lovlige formål, såsom at teste pålideligheden af informationsteknologiprodukter eller informationssystemers sikkerhed, skal der foruden kravet om et generelt forsæt også foreligge et specifikt forsæt til, at anvende disse værktøjer til at begå en eller flere af de strafbare handlinger, der er fastlagt i dette direktiv.

(17) Dette direktiv pålægger ikke strafferetligt ansvar, når de objektive kriterier for de strafbare handlinger, der er fastlagt i dette direktiv, er opfyldt, men handlingerne begås uden forsæt til at begå en strafbar handling, f.eks. når en person ikke ved, at der ikke har været givet tilladelse til adgang eller når en tilladt intervention har til formål at afprøve eller sikre informationssystemer, f.eks. når en virksomhed eller en leverandør udpeger en person til at afprøve styrken af sine sikkerhedssystemer. I forbindelse med dette direktiv bør kontraktlige forpligtelser eller aftaler om at begrænse adgang til informationssystemer ved hjælp af en brugerpolitik eller brugerbetingelser samt arbejdskonflikter vedrørende adgangen til og anvendelse af en arbejdsgivers informationssystemer til private formål ikke medføre et strafferetligt ansvar, når det under sådanne omstændigheder antages, at der ikke var givet tilladelse til adgang og dette udgør det eneste grundlag for straffesagen. Dette direktiv berører ikke retten til adgang til oplysninger, som fastsat i den nationale ret og EU-retten, men må samtidig heller ikke tjene som en begrundelse for ulovlig eller vilkårlig adgang til oplysninger.

[1] EUT L 300 af 11.11.2008, s. 42.

(18) Forskellige omstændigheder kan lette it-angreb, som f.eks. når gerningsmanden inden for rammerne af sit arbejde har adgang til sikkerhedssystemer, der indgår i de berørte informationssystemer. Der bør i den nationale ret tages passende hensyn til sådanne omstændigheder i forbindelse med en straffesag.

(19) Medlemsstaterne bør i deres nationale ret fastsætte skærpende omstændigheder i overensstemmelse med de regler, som deres retssystem fastlægger med hensyn til skærpende omstændigheder. De bør sikre, at dommerne kan tage hensyn til disse skærpende omstændigheder, når de dømmer lovovertrædere. Det påhviler dommeren at vurdere disse omstændigheder sammen med de andre faktiske forhold i den pågældende sag.

(20) Dette direktiv regulerer ikke betingelser for udøvelse af straffemyndighed med hensyn til nogen af de i direktivet omhandlede strafbare handlinger, herunder en anmeldelse foretaget af ofret på gerningsstedet, en angivelse fra den stat, hvor den strafbare handling blev begået, eller en manglende retsforfølgelse af gerningsmanden på gerningsstedet.

(21) Inden for rammerne af dette direktiv er stater og offentlige organer fortsat fuldt ud forpligtet til at sikre respekten for menneskerettighederne og de grundlæggende frihedsrettigheder i overensstemmelse med gældende internationale forpligtelser.

(22) Dette direktiv øger vigtigheden af netværk, såsom G8 eller Europarådets netværk af kontaktpunkter, der står til disposition døgnet rundt på alle ugens dage. Disse kontaktpunkter bør kunne yde effektiv bistand og derved f.eks. lette udvekslingen af tilgængelige relevante oplysninger og adgangen til teknisk rådgivning eller tilvejebringelsen af juridiske oplysninger med henblik på efterforskning eller procedurer vedrørende strafbare handlinger i forbindelse med informationssystemer og relaterede data, der involverer den anmodende medlemsstat. For at sikre netværkenes funktionsdygtighed bør hvert kontaktpunkt have kapacitet til hurtigt at kommunikere med en anden medlemsstats kontaktpunkt med støtte bl.a. fra uddannet og udrustet personale. På grund af den hastighed, hvormed der kan foretages omfattende it-angreb, bør medlemsstaterne være i stand til straks at reagere på hastende anmodninger fra netværket af kontaktpunkter. I sådanne tilfælde kan det være formålstjenligt at lade anmodningen om oplysninger ledsage af telefonisk kontakt for at sikre, at anmodningen behandles hurtigt af den anmodede medlemsstat, og at der gives en tilbagemelding inden for otte timer.

(23) Samarbejde mellem offentlige myndigheder på den ene side og den private sektor og civilsamfundet på den anden side er af stor betydning for forebyggelsen og bekæmpelsen af angreb på informationssystemer. Det er nødvendigt at fremme og forbedre samarbejdet mellem tjenesteleverandører, producenter, retshåndhævende myndigheder og retslige myndigheder, samtidig med at retsstatsprincippet respekteres fuldt ud. Dette samarbejde kan omfatte tjenesteudbyderes bistand i forbindelse med bevarelse af eventuelle beviser, tilvejebringelse af elementer, som kan bruges til at identificere gerningsmænd og, som en sidste udvej, hel eller delvis lukning i overensstemmelse med national ret og praksis, af informationssystemer og funktioner, der er blevet inficerede eller anvendt til ulovlige formål. Medlemsstaterne bør også overveje at etablere samarbejds- og partnerskabsnetværk med tjenesteleverandører og producenter til udveksling af oplysninger om strafbare handlinger, der er omfattet af dette direktivs anvendelsesområde.

(24) Der er et behov for at indsamle sammenlignelige data om de strafbare handlinger, der er fastsat i dette direktiv. Relevante data bør stilles til rådighed for de kompetente specialiserede EU-agenturer og -organer såsom Europol og ENISA i overensstemmelse med deres opgaver og informationsbehov for at få et mere fuldstændigt billede af problemet med it-kriminalitet og net- og informationssikkerhed på EU-plan og dermed bidrage til at finde mere effektive løsninger på problemet. Medlemsstaterne bør fremsende oplysninger om gerningsmændenes modus operandi til Europol og dets europæiske center for bekæmpelse af it-kriminalitet med henblik på at foretage trusselsvurderinger og strategiske analyser af it-kriminalitet i overensstemmelse med Rådets afgørelse 2009/371/RIA af 6. april 2009 om oprettelse af Den Europæiske Politienhed (Europol) ([1]). Fremsendelse af oplysninger kan fremme en bedre forståelse af aktuelle og fremtidige trusler og derved bidrage til mere relevant og målrettet beslutningstagning om bekæmpelse og forebyggelse af angreb på informationssystemer.

(25) Kommissionen bør forelægge en rapport om anvendelsen af dette direktiv og fremsætte nødvendige forslag til retsakter som kunne føre til en udvidelse af dets anvendelsesområde under hensyntagen til udviklingen inden for it-kriminalitet. Sådanne udviklinger kan omfatte teknologiske fremskridt, f.eks. sådanne som muliggør en mere effektiv håndhævelse med hensyn til angreb på informationssystemer, letter forebyggelsen af angreb eller mindsker virkningerne heraf. Med henblik herpå bør Kommissionen tage hensyn til tilgængelige analyser og rapporter udarbejdet af relevante aktører, navnlig Europol og ENISA.

(26) For at bekæmpe it-kriminalitet effektivt er det nødvendigt at øge informationssystemernes modstandsdygtighed ved at træffe relevante foranstaltninger til at beskytte dem mere effektivt mod it-angreb. Medlemsstaterne bør træffe de nødvendige foranstaltninger til at beskytte deres kritiske infrastruktur mod it-angreb og bør betragte

([1]) EUT L 121 af 15.5.2009, s. 37.

beskyttelsen af deres informationssystemer og de relaterede data som et led heri. At sikre at juridiske personer sørger for et passende niveau af beskyttelse og sikkerhed for informationssystemer, f.eks. i forbindelse med adgang til offentligt tilgængelige elektroniske kommunikationstjenester i overensstemmelse med eksisterende EU-lovgivning om privatlivets fred og elektronisk kommunikation og databeskyttelse, er et centralt led i en omfattende tilgang til effektiv bekæmpelse af it-kriminalitet. Der bør leveres et passende niveau af beskyttelse mod rimeligt identificerbare trusler og sårbarheder i overensstemmelse med den nyeste udvikling i specifikke sektorer og specifikke databehandlingssituationer. Omkostninger og byrder i forbindelse med denne beskyttelse bør stå i forhold til den eventuelle skade, som et it-angreb ville påføre de berørte personer. Medlemsstaterne tilskyndes til i national ret at træffe relevante foranstaltninger om ansvarspådragelse i tilfælde, hvor en juridisk person åbenlyst har forsømt at tilvejebringe et passende beskyttelsesniveau mod it-angreb.

(27) Betydelige mangler i og forskelle mellem medlemsstaternes lovgivning og strafferetlige procedurer om angreb på informationssystemer kan hæmme bekæmpelsen af organiseret kriminalitet og terrorisme og kan vanskeliggøre et effektivt samarbejde mellem politi og retsvæsen på dette område. Den omstændighed, at moderne informationssystemer går på tværs af landene og landegrænserne, betyder, at angreb på sådanne systemer har en grænseoverskridende dimension, hvilket understreger det presserende behov for yderligere initiativer med henblik på en indbyrdes tilnærmelse af strafferetten på området. Koordineringen af retsforfølgningen i forbindelse med tilfælde af angreb på informationssystemer bør desuden lettes ved passende gennemførelse og anvendelse af Rådets rammeafgørelse 2009/948/RIA af 30. november 2009 om forebyggelse og bilæggelse af konflikter om udøvelse af jurisdiktion i straffesager ([1]). Medlemsstaterne bør i samarbejde med Unionen ligeledes bestræbe sig på at forbedre det internationale samarbejde om informationssystemers, computernetværks og edb-datas sikkerhed. I alle internationale aftaler, der omhandler dataudveksling, bør der tages behørigt hensyn til dataoverførsels- og datalagringssikkerhed.

(28) Forbedret samarbejde mellem de kompetente retshåndhævende myndigheder og retslige myndigheder i Unionen er afgørende for en effektiv bekæmpelse af it-kriminalitet. I den forbindelse bør der tilskyndes til en øget indsats for passende uddannelse af de relevante myndigheder for at øge forståelsen af it-kriminalitet og dens følger og fremme samarbejde og udveksling af bedste praksis, f.eks. via de kompetente specialiserede EU-agenturer og -organer. Denne uddannelse bør bl.a. sigte mod at øge opmærksomheden om de forskellige nationale retssystemer, eventuelle juridiske og tekniske udfordringer ved strafferetlige efterforskninger og fordelingen af beføjelser mellem de relevante nationale myndigheder.

(29) Dette direktiv respekter menneskerettighederne og de grundlæggende frihedsrettigheder og overholder de principper, som især er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder og den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, herunder beskyttelsen af personoplysninger, retten til privatlivets fred, ytrings- og informationsfrihed, retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar samt legalitetsprincippet og princippet om proportionalitet mellem strafbar handling og straf. Dette direktiv tilsigter især at sikre, at disse rettigheder og principper respekteres fuldt ud, og skal gennemføres i overensstemmelse hermed.

(30) Beskyttelsen af personoplysninger er, i henhold til artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde og artikel 8 i chartret om grundlæggede rettigheder, en grundlæggende rettighed. Derfor bør enhver behandling af personoplysninger i forbindelse med gennemførelsen af dette direktiv fuldt ud overholde relevant EU-ret om databeskyttelse.

(31) I medfør af artikel 3 i protokollen om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, har disse medlemsstater meddelt, at de ønsker at deltage i vedtagelsen og anvendelsen af dette direktiv.

(32) I medfør af artikel 1 og 2 i protokollen om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, deltager Danmark ikke i vedtagelsen af dette direktiv, som ikke er bindende for og ikke finder anvendelse i Danmark.

(33) Målene for dette direktiv, nemlig at underkaste angreb på informationssystemer i alle medlemsstaterne strafferetlige sanktioner, der er effektive, står i et rimeligt forhold til de strafbare handlingers grovhed og har afskrækkende virkning, og at forbedre og fremme samarbejdet mellem retslige og andre kompetente myndigheder, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor på grund af deres omfang eller virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(34) Dette direktiv sigter mod at ændre og udvide bestemmelserne i Rådets rammeafgørelse 2005/222/RIA af 24. februar 2005 om angreb på informationssystemer ([2]). Eftersom de ændringer, der skal foretages, er væsentlige, både hvad angår antal og karakter, bør rammeafgørelse 2005/222/RIA af hensyn til klarheden erstattes i sin helhed i forhold til de medlemsstater, der deltager i vedtagelsen af dette direktiv —

([1]) EUT L 238 af 15.12.2009, s. 42.

([2]) EUT L 69 af 16.3.2005, s. 67.

VEDTAGET DETTE DIREKTIV:

*Artikel 1*

**Genstand**

Dette direktiv fastsætter minimumsregler vedrørende definitionen af strafbare handlinger og sanktioner i forbindelse med angreb på informationssystemer. Det sigter endvidere mod at lette forebyggelsen af sådanne strafbare handlinger og forbedre samarbejdet mellem retslige og andre kompetente myndigheder.

*Artikel 2*

**Definitioner**

I dette direktiv forstås ved:

a) »informationssystem«: enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program, som automatisk behandler edb-data, samt edb-data, som lagres, behandles, fremfindes eller overføres af denne enhed eller gruppe af enheder i forbindelse med dens eller deres drift, brug, beskyttelse og vedligeholdelse

b) »edb-data«: enhver form for gengivelse af fakta, informationer eller begreber i et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få et informationssystem til at udføre en funktion

c) »juridisk person«: en enhed, der har status som juridisk person i henhold til den lovgivning, der finder anvendelse, med undtagelse af stater eller offentlige organer, der udøver deres statsmyndighed, eller offentlige internationale organisationer

d) »uretmæssig«: adfærd som omhandlet i dette direktiv, herunder adgang, indgreb eller opfangning, som ejeren eller en anden rettighedsindehaver af systemet eller en del af det ikke har givet tilladelse til, eller som ikke er tilladt i henhold til national lovgivning.

*Artikel 3*

**Ulovlig adgang til informationssystemer**

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt at skaffe sig uretmæssig adgang til et informationssystem eller en del heraf, når den strafbare handling er begået ved brud på en sikkerhedsforanstaltning, i det mindste i grovere tilfælde.

*Artikel 4*

**Ulovligt indgreb i informationssystemer**

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt og uretmæssigt at forårsage en alvorlig hindring eller afbrydelse af et informationssystems drift ved at indlæse edb-data, overføre, beskadige, slette, forvanske, ændre eller tilbageholde sådanne data eller at gøre sådanne data utilgængelige, i det mindste i grovere tilfælde.

*Artikel 5*

**Ulovligt indgreb i data**

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt og uretmæssigt at slette, beskadige, forvanske, ændre eller tilbageholde edb-data i et informationssystem eller at gøre sådanne data utilgængelige, i det mindste i grovere tilfælde.

*Artikel 6*

**Ulovlig opfangning**

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at det er strafbart forsætligt og uretmæssigt ved hjælp af tekniske hjælpemidler at opfange ikke-offentlige overførsler af edb-data til, fra eller inden for et informationssystem, herunder elektromagnetisk udsending fra et informationssystem, der indeholder disse edb-data, i det mindste i grovere tilfælde.

*Artikel 7*

**Værktøjer, der anvendes til at begå strafbare handlinger**

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at det er strafbart bevidst at fremstille, sælge, erhverve med henblik på brug, importere, distribuere eller på anden måde stille et af følgende værktøjer til rådighed uretmæssigt og med forsæt til, at det anvendes til at begå en af de strafbare handlinger i artikel 3-6, i det mindste i grovere tilfælde:

a) et edb-program, der hovedsagelig er beregnet eller tilpasset til at begå en af de strafbare handlinger i artikel 3-6

b) edb-password, adgangskoder eller tilsvarende data, hvorved der kan opnås adgang til et helt informationssystem eller en del heraf.

*Artikel 8*

**Anstiftelse, medvirken og tilskyndelse samt forsøg**

1. Medlemsstaterne sikrer, at det er strafbart at anstifte eller medvirke og tilskynde til at begå en strafbar handling som omhandlet i artikel 3-7.

2. Medlemsstaterne sikrer, at det er strafbart at forsøge at begå en strafbar handling som omhandlet i artikel 4 og 5.

*Artikel 9*

**Sanktioner**

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-8 kan straffes med strafferetlige sanktioner, der er effektive, står i et rimeligt forhold til den strafbare handlings grovhed og har afskrækkende virkning.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-7 kan straffes med fængsel med en maksimumstraf på mindst to år, i det mindste i grovere tilfælde.

3. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 4 og 5, kan straffes med fængsel med en maksimumsstraf på mindst tre år, når de begås forsætligt, og når et betydeligt antal informationssystemer

er blevet berørt gennem anvendelsen af et af værktøjerne i artikel 7, der hovedsagelig er udarbejdet eller tilpasset til dette formål.

4. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 4 og 5 kan straffes med fængsel med en maksimumsstraf på mindst fem år, når:

a) de er begået inden for rammerne af en kriminel organisation som defineret i rammeafgørelse 2008/841/RIA uanset den deri fastsatte straf

b) de forvolder alvorlig skade, eller

c) de er begået mod et kritisk infrastruktur-informationssystem.

5. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at når de strafbare handlinger i artikel 4 og 5 begås ved at misbruge en anden persons personoplysninger med det formål at vinde tredjemands tillid og derved skade den, som identiteten egentlig tilhører, kan det, i overensstemmelse med national ret, betragtes som skærpende omstændigheder, medmindre disse omstændigheder allerede er omfattet af en anden handling, der er strafbar i henhold til national ret.

*Artikel 10*

**Juridiske personers ansvar**

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at juridiske personer kan drages til ansvar for de i artikel 3-8 omhandlede strafbare handlinger, som for at skaffe dem vinding begås af en person, der handler enten individuelt eller som medlem af et organ under den juridiske person, og som har en ledende stilling inden for den juridiske person baseret på et af følgende forhold:

a) en beføjelse til at repræsentere den juridiske person

b) en bemyndigelse til at træffe beslutninger på den juridiske persons vegne

c) en bemyndigelse til at udøve intern kontrol inden for den juridiske person.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at den juridiske person kan drages til ansvar, hvis manglende tilsyn eller kontrol fra en af de i stk. 1 omhandlede personers side har gjort det muligt for en person, der er underlagt den juridiske persons myndighed, at begå nogen af de i artikel 3-8 omhandlede strafbare handlinger med henblik på at skaffe den juridiske person vinding.

3. Juridiske personers ansvar i henhold til stk. 1 og 2 udelukker ikke strafferetlig retsforfølgning af fysiske personer, der begår eller anstifter eller medvirker til nogen af de i artikel 3-8 omhandlede strafbare handlinger.

*Artikel 11*

**Sanktioner over for juridiske personer**

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at juridiske personer, der kendes ansvarlige i henhold til artikel 10, stk. 1, kan straffes med sanktioner, der er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning, som omfatter strafferetlige og andre bøder og som kan omfatte andre sanktioner såsom:

a) udelukkelse fra offentlige ydelser eller tilskud

b) midlertidigt eller varigt forbud mod at udøve erhvervsvirksomhed

c) anbringelse under retsligt tilsyn

d) tvangsopløsning efter retskendelse

e) midlertidig eller permanent lukning af forretningssteder, der er blevet brugt til at begå den strafbare handling.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at juridiske personer, der kendes ansvarlige i henhold til artikel 10, stk. 2, kan straffes med sanktioner eller andre foranstaltninger, der er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning.

*Artikel 12*

**Straffemyndighed**

1. Hver medlemsstat fastlægger sin straffemyndighed med hensyn til de i artikel 3-8 omhandlede strafbare handlinger, når den strafbare handling er begået:

a) helt eller delvis på dens område, eller

b) af en af dens statsborgere, i det mindste i de tilfælde, hvor handlingen er en strafbar handling dér, hvor den blev begået.

2. Når en medlemsstat fastlægger sin straffemyndighed i overensstemmelse med stk. 1, litra a), sikrer den sig, at dens straffemyndighed omfatter tilfælde, hvor:

a) gerningsmanden begår den strafbare handling, mens vedkommende fysisk befinder sig på dens område, uanset om den strafbare handling er rettet mod et informationssystem på dens område, eller

b) den strafbare handling begås mod et informationssystem på dens område, uanset om gerningsmanden på gerningstidspunktet fysisk befinder sig på dens område.

3. En medlemsstat underretter Kommissionen, hvis den beslutter at fastlægge straffemyndighed med hensyn til en af de i artikel 3-8 omhandlede strafbare handlinger, som er begået uden for dens område, herunder når:

a) gerningsmanden har sit sædvanlige opholdssted på dens område, eller

b) den strafbare handling er begået til fordel for en juridisk person, som har sit hjemsted på dens område.

*Artikel 13*

**Udveksling af oplysninger**

1. Med henblik på udveksling af oplysninger om de i artikel 3-8 omhandlede strafbare handlinger, sikrer medlemsstaterne, at de har et funktionsdygtigt nationalt kontaktpunkt, og at de gør brug af det bestående netværk af kontaktpunkter, der står til disposition døgnet rundt på alle ugens dage. Medlemsstaterne sikrer endvidere, at der findes procedurer, så den kompetente myndighed i forbindelse med hasteanmodninger om hjælp inden for otte timer fra modtagelsen kan angive som minimum, om anmodningen vil blive imødekommet, samt på hvilken måde og på hvilket tidspunkt dette forventes at ske.

2. Medlemsstaterne underretter Kommissionen om deres udpegede kontaktpunkt, som omhandlet i stk. 1. Kommissionen videresender oplysningerne til de øvrige medlemsstater og kompetente specialiserede EU-agenturer og -organer.

3. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at der stilles passende anmeldelseskanaler til rådighed med henblik på at lette anmeldelse uden unødige forsinkelser til de kompetente nationale myndigheder om de i artikel 3-6 omhandlede strafbare handlinger.

*Artikel 14*

**Overvågning og statistik**

1. Medlemsstaterne sikrer, at der findes et system til registrering, fremstilling og fremlæggelse af statistiske oplysninger om de i artikel 3–7 omhandlede strafbare handlinger.

2. De statistiske oplysninger i stk. 1 skal mindst omfatte de eksisterende oplysninger om det antal strafbare handlinger, der henvises til i artikel 3-7, som er registreret i medlemsstaterne, og det antal personer, der er blevet retsforfulgt og dømt for de i artikel 3-7 omhandlede strafbare handlinger.

3. Medlemsstaterne fremsender de oplysninger, der er indsamlet i henhold til denne artikel, til Kommissionen. Kommissionen sikrer, at der offentliggøres en konsolideret oversigt over disse statistiske rapporter, og at denne fremsendes til de kompetente specialiserede EU-agenturer og -organer.

*Artikel 15*

**Erstatning af rammeafgørelse 2005/222/RIA**

Rammeafgørelse 2005/222/RIA erstattes hermed i forhold til de medlemsstater, der deltager i vedtagelsen af dette direktiv, uden at det berører medlemsstaternes forpligtelser for så vidt angår fristerne for gennemførelse af rammeafgørelsen i national ret.

I forhold til de medlemsstater, der deltager i vedtagelsen af dette direktiv, gælder henvisninger til rammeafgørelse 2005/222/RIA som henvisninger til dette direktiv.

*Artikel 16*

**Gennemførelse**

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest 4. september 2015.

2. Medlemsstaterne meddeler Kommissionen teksten til de love og bestemmelser, som gennemfører de forpligtelser, der pålægges dem i medfør af dette direktiv, i deres nationale lovgivning.

3. Disse love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

*Artikel 17*

**Rapportering**

Kommissionen forelægger senest den 4. september 2017 en rapport for Europa-Parlamentet og Rådet med en vurdering af, i hvilket omfang medlemsstaterne har truffet de nødvendige foranstaltninger til at efterkomme dette direktiv, om nødvendigt ledsaget af lovgivningsmæssige forslag. Kommissionen tager også hensyn til den tekniske og lovgivningsmæssige udvikling inden for it-kriminalitet, navnlig med hensyn til dette direktivs anvendelsesområde.

*Artikel 18*

**Ikrafttræden**

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

*Artikel 19*

**Adressater**

Dette direktiv er rettet til medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den 12. august 2013.

| *På Europa-Parlamentets vegne* | *På Rådets vegne* |
|---|---|
| M. SCHULZ | L. LINKEVIČIUS |
| *Formand* | *Formand* |